IPS 1-17 Information Security Program

Effective Date: May 9, 2018
Responsible Office: Office of the Chief Information Officer (OCIO)
Supersedes: 06/16/17; MS 542 01/07/13; 07/19/12; 01/26/06; 05/21/02; 06/16/88

Transmittal Memo MS 542
Issuance Memo (07/19/2012)
Issuance Memo (01/07/2013)
Issuance Memo (06/16/2017)
Issuance Memo (05/09/2018)

IPS 1-17 *Information Security Control Catalog*
IPS 1-17 *Rules of Behavior - General*
IPS 1-17 *Rules of Behavior - Privileged*

1.0 Purpose

This Manual Section sets forth the Peace Corps Information Security Program (Program), which addresses information security for the Peace Corps **unclassified** information systems.

2.0 Authorities

The Freedom of Information Act (FOIA), 5 U.S.C. 552; Presidential Memorandum on the FOIA, January 21, 2009; Records Management Act, 44 U.S.C. 31; E-Government Act of 2002, 44 U.S.C. 101; Federal Information Security Modernization Act of 2014 (FISMA); National Institute of Standards and Technology (NIST) Special Publications; Office of Management and Budget (OMB) Circulars and Memoranda, and Federal Information Processing Standards (FIPS) Publications, Executive Order 13556 "Controlled Unclassified Information", Executive Order 13800 "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure", including FIPS Publication 200; Federal Information Technology Acquisition Reform Act (FITARA), Pub. L. No. 113-291 and related information technology management guidance.

3.0 Applicability

The Peace Corps requires that all information systems (regardless of location or delivery mechanism) abide by the security policies set forth in this Program to ensure the confidentiality, integrity, and availability of data in Peace Corps information systems. The Federal Government has instituted a number of laws, regulations, and directives that govern the establishment and implementation of federal information security practices. These laws, regulations, and directives establish federal and agency-level responsibilities for information security, define key information security roles and responsibilities, identify minimum information security controls, specify compliance with reporting rules and procedures, and provide other essential requirements and guidance. These laws and regulations place responsibility and accountability for information security at all levels within federal agencies, from agency heads to the information technology users.

Additionally, the policies defined within are designed to facilitate commonality in the planning, implementing, monitoring, and reporting of security requirements and to be used as a reference by information system owners, project managers, and other responsible federal and contractor staff. These policies are organized around the control families defined in *NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations*.

The Program sets the policy direction for safeguarding electronic information and information systems from various threats while demonstrating successful program stewardship to the Federal Government. It also enables Peace Corps information assets to be protected in a manner commensurate with mission importance, threat environments, known vulnerabilities, and consequence of loss for the information it processes. This Program also puts in place the guidelines that:

(a) Establishes the risk management framework (RMF) aligned with NIST Special Publication 800-39, Managing Information Security Risk Organization, Mission, and Information System View and the latest version of NIST Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.

(b) Protects Peace Corps information and information assets in a cost effective manner by managing information security risks, considering mission priorities, and allocating resources to the most efficient solutions necessary to reduce risk to acceptable levels.

(c) Takes into account the need to synchronize mission execution and performance with business, information technology (IT) infrastructure, and security requirements.

(d) Provides the flexibility to tailor and implement risk mitigation controls in light of threats, acceptable risks, mission needs, and environmental and operational factors.

(e) Integrates Enterprise Architecture standards, principles, and guidelines with information security.

(f) Incorporates privacy requirements.

4.0 Definitions

(a) ***Availability*** is ensuring timely and reliable access to and use of information.

(b) ***Cyber Security Assessment and Management*** **(CSAM)** *is the system of records for documentation and artifacts related to the assessment and authorization of Peace Corps information systems.*

(c) ***Cloud Services*** are any service made available to users on demand via the Internet from a cloud computing provider's servers as opposed to being provided from a Peace Corps owned on-premises server(s). Cloud Services and related systems to be used by the Peace Corps require a full IT security assessment prior to transferring Peace Corps data to these systems. Only Cloud Services expressly approved in writing by OCIO are permissible for use by Peace Corps staff and other users of Peace Corps IT information systems and hardware.

(d) ***Common Control*** is a security control that is inheritable by one or more organizational information systems.

(e) ***Common Control Provider*** is an individual, group, or organization responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems. Common control providers are responsible for: (i) documenting the organizational-identified common controls in a security plan; (ii) ensuring that required assessments of common controls are carried out by qualified assessors with an appropriate level of independence defined by the organization; (iii) documenting assessment findings in a security assessment report; and (iv) producing a plan of action and milestones for all controls having weaknesses or deficiencies.

(f) ***Confidentiality*** is preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary or sensitive information.

(g) ***Cybersecurity & Policy Catalog*** is a document that provides detail on how security controls must be implemented at the Peace Corps.

(h) ***Encryption*** is the process of converting plaintext into cipher text for the purpose of security or privacy.

(i) ***General User*** is any person accessing a Peace Corps information system or application either from the Peace Corps domain (internal user) or from the Internet (external user). The general user is the consumer of any Peace Corps products or services provided by a Peace Corps information system and are only granted privileges required to access the product or service provided by the Peace Corps information system.

(j) ***Information System*** is a discrete set of information resources, hardware and/or software, owned and operated by or on the behalf of the Peace Corps, which are organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of Peace Corps **unclassified** information.

(k) ***Integrity*** is guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

(l) ***Organizationally Defined Parameters*** **(ODP)** are values that give organizations the flexibility to define selected portions of the security controls to support specific organizational requirements or objectives.

(m) ***Plan of Action and Milestones*** **(POA&M)** is a process that identifies tasks that need to be accomplished. It details tasks required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist Peace Corps in identifying, prioritizing, and monitoring the progress of corrective actions for security weaknesses found in programs and systems.

(n) ***Potential Impact Levels (FIPS 199)*** are the potential impact on the organization or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The impact levels are:

LOW: Information is considered low impact if loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: Exposure of a user name and business email can cause limited adverse effect meaning that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

MODERATE: information is considered moderate impact if loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: Exposure of a user's name and financial information (e.g., social security number) can have a serious adverse effect meaning that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

HIGH: Information is considered high impact if loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: Exposure of highly sensitive information (e.g., accusatory information such as allegations of sexual misconduct) can have a severe or catastrophic adverse effect meaning that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

(o) ***Privileged User*** is a user who has been allocated powers within the network and/or information system, which are significantly greater than those available to the General User and can be used to circumvent security safeguards and established business processes. (See section 5.13 for additional information.)

(p) ***Publicly Accessible Websites and Services*** are online resources and services available over HTTP or HTTPS over the public internet that are operated and maintained in whole or in part by the Peace Corps, contractor, or other organization on behalf of the Peace Corps. They present government information or provide services to the public or a specific user group and support the performance of an agency's mission. This definition includes all web interactions, whether a visitor is logged-in or anonymous.

(q) ***Risk*** is the probability of damage, injury, liability, loss, or any other negative effect that is caused by a threat agent exploiting a technical, procedural, or organizational (i.e., lack of resources or management oversight) weakness or vulnerability.

(r) ***Risk Management*** is the process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation of an information system. This includes assessing **unclassified** information system risks, implementing risk mitigation strategy, and employing continuous monitoring to consistently assess the security state of the information system.

(s) ***Security, Policy, and Governance*** **(SP&G)** is the OCIO group responsible for the development, implementation and maintenance of the Peace Corps **unclassified** Information Security Program.

(t) ***Security Assessment and Authorization*** **(SA&A)** is the process of conducting a security assessment on a system and determining, based on the results of that assessment, whether the system should be given a security authorization.

(u) ***Security Authorization*** is the notice to proceed with the "live" system. It is the official management decision given by the Authorizing Official to authorize operation of an information system and to explicitly accept the risk to Peace Corps operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. Security Authorizations are also referred to as an "Authorization to Process" or "Authority to Operate (ATO)."

(v) ***Sensitive Information*** is information that if obtained, exposed or distributed by unauthorized individuals can cause harm to the Peace Corps' workforce, assets or reputation. Examples of sensitive data are, but are not limited to: Personally Identifiable Information (PII); electronic Personal Health Information (ePHI); financial information; and information labeled For Official Use Only (FOUO), Internal Use, Sensitive but Unclassified (SBU) or Controlled Unclassified Information (CUI).

(w) ***System Authorization Boundary*** is a description or diagram that includes all components of an information system to be authorized for operation by the authorizing official and excludes separately authorized systems to which the information system is connected.

(x) ***Third Party Collaboration Tool*** is a cloud service used to support a group of two or more individuals to accomplish a common goal or objective they have set themselves.

(y) ***Vulnerability*** is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

5.0 Roles and Responsibilities

5.1 Peace Corps Director

The Director has the overall responsibility to provide information security protections commensurate with the risk and magnitude or impact of harm to organizational operations and assets, individuals, other organizations that may result from unauthorized access, use, disclosure, disruption, modification, or destruction of: (i) information collected or maintained by or on behalf of the Peace Corps; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

5.2 Authorizing Official

The Chief Information Officer (CIO) is the Authorizing Official for Peace Corps information systems. The Authorizing Official has the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, assets, or individuals. Through the security authorization process, the authorizing official is accountable for the security risks associated with information system operations. Accordingly, the authorizing official is in a management position with a level of authority commensurate with understanding and accepting such information system-related security risks. The Authorizing Official cannot also be the System Owner for a system operating under his/her authority.

The Authorizing Official must complete role based security training prior to executing any signatory responsibilities as the Authorizing Official.

The Authorizing Official may approve or deny authorization to operate (ATO) for an information system. If the system is operational, the Authorizing Official may halt operations when unacceptable risks exist. The Authorizing Official coordinates activities with the risk executive (function), Chief Information Security Officer, System Owners, Information System Security Managers, security control assessors, and other interested parties during the security authorization process.

5.3 Chief Information Officer

The Chief Information Officer (CIO) promotes and coordinates the agency-wide information security program; assigns a Chief Information Security Officer to develop and implement the Program; and manages the OCIO, which is the agency’s common control provider for information security policies and procedures. (Note: The Office of Safety and Security is the common control provider for physical and personnel security controls, while the Office of Management is the common control provider for environmental controls.)

5.4 Chief Information Security Officer

The Chief Information Security Officer (CISO) is an OCIO official responsible for: (i) carrying out the CIO's security responsibilities under FISMA; and (ii) serving as the primary liaison to information system owners, common control providers, and information system security managers for the CIO on matters related to Peace Corps' Information Security Program and, **unclassified** information security policies and procedures. The CISO:

(a) Develops, documents, and implements an agency-wide IT security program to provide information security for the information and information systems that support the operations and assets of the agency in the most cost-effective manner.

(b) Ensures departments are informed on total cost of ownership requirements required to support this Directive in a timely manner to support resource justifications.

(c) Develops and maintains information security policies, procedures, and control techniques to address all applicable requirements for protecting Peace Corps information and information systems.

(d) Assists senior Peace Corps officials in performing their information security responsibilities.

(e) Develops, maintains, authorizes, and manages a Peace Corps information system risk management framework.

(f) Manages the Enterprise Common Controls and associated organizationally defined parameters on behalf of the agency.

(g) Reviews and approves cybersecurity policy deviations where appropriate.

(h) Provides mandatory computer security training for Peace Corps employees and contractors, at the time of hiring/onboarding and on an annual basis, to make them aware of the policies and procedures for protecting sensitive information.

5.5 Associate Director of the Office of Safety and Security

The Associate Director of the Office of Safety and Security coordinates continuity of operations and insider threat planning and activities with the OCIO to ensure that business processes and information systems used to support business processes are documented as required to support each individual plan.

5.6 Risk Executive (Function)

The Deputy Director, or designated delegates, serves as Risk Executive and provides comprehensive, organization wide approach to risk management; serves as the common risk management resource for senior leaders/executives, system owners, CIO, CISO, information security officer, information system owners, common control providers; information system security managers, and stakeholders in the system success of the agency.

5.7 Information Owner

The information owner is an organizational official with statutory, management, or operational authority for specified information and the responsibility for establishing the policies and procedures governing its generation, collection, processing, dissemination, storage, and disposal. The information owner, with the support of the ISSM and OCIO technical resources, is responsible for establishing the rules for appropriate use and protection of the subject information and retains that responsibility even when the information is shared outside the agency. The owner of the information processed, stored, or transmitted by an information system may or may not be the same as the system owner. A single information system may contain information from multiple information owners. Information owners provide input to information system owners regarding the security requirements and security controls for the systems where the information is processed, stored, or transmitted. The information owner may work in concert with the system owner or information system owner, and the ISSM or the Privacy Office to complete the FIPS 199 categorization and/or the Privacy Threshold Analysis and Privacy Impact Assessment as required for the Risk Management Framework process.

5.8 System Owner

Each Peace Corp information system must have a System Owner (SO) throughout the information system’s lifecycle. The designation should be made by the leadership within the information system’s sponsoring business unit. The SO, with the support of the ISSM and OCIO technical resources, is responsible for the planning, development, operation, maintenance and disposition of information systems used to support Peace Corps business processes. In particular, the SO is accountable for the development and maintenance of the security plan and ensures that the system is deployed and operated in accordance with the agreed-upon security controls. With assistance from OCIO as needed, the SO will support the implementation and function of information system security controls throughout the information system’s lifecycle.

SOs must complete Peace Corps role based security training prior to executing any signatory responsibilities as the System Owner.

5.9 Information System Security Manager

The Information System Security Manager (ISSM) is responsible for ensuring the appropriate security posture is established and maintained throughout the information system’s lifecycle. The ISSM is selected by and reports to the CISO. The information system security manager works in close collaboration with the information system owner and stakeholders and serves as a principal advisor on all matters, technical and otherwise, involving the security of an information system. The information system security manager must have detailed knowledge and expertise required to manage the security aspects of an information system and is assigned the responsibility for the day-to-day security operations of a system. Such positions are assigned by and report directly to the CISO.

5.10 Information System Security Officer (ISSO)

The ISSO will support the SO, Business Owner or Product Owner in his/her area of responsibility in the implementation of the Risk Management Framework and Enterprise Risk

Management. The ISSO is responsible for ensuring that the ISs, software services (SaaS) and major applications meet federal and Agency requirements for the implementation of RMF, that there is a level of security consistent with Peace Corps' risk-based approach, and that security effectively and efficiently supports the business mission. The ISSO should become familiar with other Agency ISSOs to collaborate and share ideas.

With oversight and guidance from the ISSM, the ISSO serves as the principal advisor to the SO and the CISO on all matters involving the security of the IS. The ISSO is responsible for ensuring that the appropriate operational security posture is maintained for an IS and works in close collaboration SO. The ISSO typically has the detailed knowledge and expertise required to manage the security aspects of the IS and, in many cases, are assigned responsibility for the day-to-day security operations of the system.

Though the ISSO performs security functions, the SO maintains overall responsibility for IS security. The ISSO may be called upon to assist in the development of the system security policy and to ensure compliance with the policy on a routine basis. In coordination with the SO, the ISSO often plays an active role in the SA&A process and continuous monitoring activities, such as developing and updating the SP; managing and controlling changes to the system and assessing the security impact of those changes; and POA&M management. ISSOs also coordinate with external agencies and assist in the preparation of ISAs to ensure all external connections meet protection requirements and are documented in the SP, Risk Assessment, and security operating procedures.

At a minimum an ISSO, along with an SO and an AO, must be designated for every major application, IS, and General Support System (GSS), including cloud-based systems. These roles serve as the primary contacts for all security matters related to those systems.

5.11 Security Control Assessor

The security control assessor (SCA) is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls. The SCA is selected by and reports to the CISO. SCAs are additionally responsible for:

(a) Providing an assessment of the severity of weaknesses and recommend corrective actions to address identified vulnerabilities; and

(b) Preparing the final security assessment report containing the results and findings from the assessment.

5.12 General Users

General Users must:

(a) Review and sign the IPS 1-17 *Rules of Behavior for General Users* as a condition of access to the Peace Corps network and sign the *New User's Verification Form* (PC-1780).

(b) Complete required information security awareness training prior to gaining access to the Peace Corps network domain and **unclassified** information systems.

5.13 Privileged Users

In addition to the responsibilities identified for General Users, Privileged Users must:

(a) Review the Peace Corps IPS 1-17 *Rules of Behavior for Privileged Users* and sign and get the required authorized signatures on the *Privileged User Account Request Form* (PC-2076-e);

(b) Complete required information security and functional training before using their privileged account. See Peace Corps Role Based IT Security Training: Plan and Procedures, June 30, 2017, version 1.4 for detailed roles, responsibility and training requirements.

6.0 Cybersecurity and Privacy Control Policies

Information systems that process, store, or transmit Peace Corps data shall comply with all cybersecurity policies and applicable procedures listed in the Peace Corps Cybersecurity and Privacy Catalog.

6.1 Cybersecurity Control Policies

6.1.1 Access Control (AC) Policy

In accordance with the AC Control system baseline defined by the system's categorization, system owner with the support of the ISSO will:

(a) Ensure access to IT Resources are commensurate with the categorization of the data it processes;

(b) Define an access enforcement process that limits logical access to approved authorized users based on the system’s mission requirements;

(c) Control the flow of information within the system and between interconnected systems based on the principles of need-to-know and least privilege;

(d) Enforce separation of duties to minimize the potential of abuse of authorized privileges and help reduce the risk of malicious activity without collusion;

(e) Employ least privilege to a degree that allows only authorized access for users (or processes acting on behalf of the user) which are necessary to accomplish assigned tasks in accordance with the mission or business function of the system;

(f) Control unsuccessful logon attempts and maintain records of such attempts that are adequate for Incident Response investigations (legacy systems may be exempt from this policy);

(g) Restrict concurrent logon sessions to the minimal number required based on the system’s mission requirements;

(h) Control inactive users sessions through session locking and termination based on the mission or business functions of the system;

(i) Limit user or process actions without identification or authentication and document all exceptions as risks in the systems security documentation;

(j) Ensure that security attributes associations (metadata) are made and retained with information to control access across system components;

(k) Document the terms and conditions for the access or exchange of information to external entities or internal entities outside the system accreditation bounty;

(l) In cases where information is disseminated to the public, define a process for decimating public information that is compliance with Agency policy and establish logical controls to ensure that process is enforced;

(m) Ensure all access is attributed to a single known individual or process. Anonymous access should only be used to facilitate access to public data. The use of shared credentials to access non-public systems is strictly prohibited.

6.1.2 Awareness and Training (AT) Policy

Peace Corps will conduct Peace Corps-wide security awareness training, in addition to role-based training for privileged or elevated users, at least annually in accordance with all applicable Laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of Peace Corps’ information systems and data to include digital and paper assets. Peace Corps will maintain security training records for all users who complete this training and make that information available to system owners.

In accordance with the AT Control baseline defined by the system’s categorization, the SP&G Security Awareness and Training Manager, on behalf of System Owners, will:

(a) Ensure their user base are aware of all system specific security process and procedures;

(b) Ensure all authorized users have received initial cybersecurity and privacy awareness training as a condition of access, and thereafter have completed the Peace Corps annual cybersecurity and privacy awareness refresher training. Organizational security awareness training is mandatory as a condition of user access to Peace Corps systems.

(c) Ensure Peace Corps personnel are adequately trained to carry out assigned cybersecurity and privacy duties based on the roles they are assigned;

(d) Maintain training records for any system specific training that is required.

6.1.3 Audit and Accountability (AU) Policy

Information systems that process, store, or transmit Peace Corps data will comply, through common control inheritance or direct implementation, with the security controls and applicable procedures listed in the Peace Corps Cybersecurity and Privacy Catalog.

In accordance with the AU Control baseline defined by the system's categorization, ISSOs, in support of system owners, will:

(a) Create, protect, and retain system audit records to the extent needed to enable security monitoring, analysis, investigation and reporting of unlawful, unauthorized or inappropriate system activity;

(b) Ensure the actions are attributable to an individual user or process that can be uniquely traced;

(c) Ensure audit capacity is adequate to support event retention requirements;

(d) Ensure procedures are in place to address audit processing failures;

(e) Provide direct, real-time or near real-time electronic data feeds of all relevant security monitoring and event data (e.g., Firewall event logs, Intrusion Detection and/or Prevention system alerts and logs, network and desktop antivirus event logs, content scanning and filtering system logs, DHCP, DNS, etc.) to an appropriate Peace Corps data collector.

(f) Review system specific audit reports for anomalies;

(g) Ensure audit information protections are in place to prevent unauthorized access or modification of audit records.

6.1.4 Security Assessment and Authorization (CA) Policy

In accordance with the CA Control baseline defined by the system's categorization, ISSOs, in support of system owners, will:

(a) Conduct assessments in accordance with ISSO Handbook, Risk Management Framework (RMF) Steps 1 through 5;

(b) Document all System Interconnections (Internal and External) and in accordance with agency policies and procedures;

(c) Maintain timely and accurate Plan of Action and Milestones documentation;

(d) Ensure all mission and business systems have current security authorizations signed by the appropriate Authorizing Officials;

(e) Integrate system process and procedures into the Agency continuous monitoring framework.

All pertinent Security Assessment and Authorization documents and supporting artifacts will be maintained in CSAM.

6.1.5 Configuration Management (CM) Policy

SP&G will participate in the Change Control Board to identify changes that have a significant impact on security controls. A re-assessment of security control may be required if the change significantly impacts the effectiveness or function of the security baseline.

In accordance with the CM Control baseline defined by the system’s categorization, infrastructure service provider will:

(a) Establish system and component baseline configuration settings and ensure that a current baseline configuration is implemented and maintain for each system;

(b) Ensure that all systems have a Change Management Plan and participate in the appropriate Change Management process;

(c) Ensure that all changes undergo security impact analysis;

(d) Enforce physical and logical access restriction to limit unauthorized system changes;

(e) Configure systems to comply with the principle of Least Functionality and disable or remove unnecessary components (software or hardware);

(f) Maintain a current and accurate information system component inventory and adequate licensing for all components.

6.1.6 Contingency Planning (CP) Policy

In accordance with the CP Control baseline defined by the system’s categorization, ISSOs, in support of System Owners, will:

(a) Maintain a current and accurate contingency plan that is adequate to meet mission requirements and is reviewed, tested and updated at least annually;

(b) Ensure all individuals assigned to contingency roles have adequate training to perform their duties;

(c) Monitor system recovery technical controls for compliance with the system contingency plan and perform regular tests to ensure recovery data is available and adequate to successfully conduct recovery and reconstitution operations.

6.1.7 Identification and Authentication (IA) Policy

In accordance with the IA Control baseline defined by the system’s categorization, ISSOs, in support of System Owners, will:

(a) Uniquely identify and authenticate all users, devices or services to systems that require restricted or named access;

(b) Adhere to Peace Corps Cybersecurity and Privacy Catalog for Access Control Processes.

6.1.8 Incident Response (IR) Policy

Peace Corps will maintain an enterprise-wide incident response process. System Owners will:

(a) Adhere to Peace Corps Incident Response Plan, January 2018;

(b) Establish and maintain system and mission level incident response plan and process that address incident handling at the system and mission level;

(c) Ensure that are incident response roles are trained to perform their assigned duties;

(d) Conduct an annual incident response test to evaluate the effectiveness of the incident response process and document the results;

(e) Report incidents to the appropriate authorities in accordance with the Agency Incident Response process.

6.1.9 Maintenance (MA) Policy

In accordance with the MA Control baseline defined by the system’s categorization, ISSOs, in support of System Owners, will:

(a) Ensure all types of system maintenance activities are documented and approved in accordance with Peace Corps Cybersecurity and Privacy Catalog;

(b) Ensure all maintenance personnel are properly vetted and adequately trained to conduct maintenance operations;

(c) Ensure that maintenance is conducted in a timely manner and potentially impacted security controls are test for effectiveness as part of the maintenance implementation plan.

6.1.10 Media Protection (MP) Policy

In accordance with the MP Control baseline defined by the system’s categorization, ISSOs, in support of System Owners, will:

(a) Restrict all media access, transport and storage to authorized personnel in accordance with Peace Corps policies and procedures;

(b) Mark all media in accordance with the applicable Peace Corps Information Security handbook based on the media type;

(c) Handle and control all media based on the potential impact level of the unclassified data it contains;

(d) Sanitize media prior to disposal in accordance with Peace Corps policies and procedures.

6.1.11 Physical and Environmental Protection (PE) Policy

In accordance with the PE Control baseline defined by the system's categorization, ISSOs, in support of System Owners, will:

(a) Maintain a list of individuals authorized to access the physical system;

(b) Implement the appropriate physical access controls when within the scope of the system boundary;

(c) Monitor physical access when within the scope of the system boundary;

(d) Control visitor access to physical systems and ensure all visitor access is monitored;

(e) Track all physical assets and ensure that location records are current and accurate;

6.1.12 Planning (PL) Policy

In accordance with the PL Control baseline defined by the system's categorization, ISSOs, in support of System Owners, will:

(a) Develop and maintain a system security plan that relate the security requirements of the system and describe, at a high level, how the security controls and enhancements meet those security requirements;

(b) Establish system specific rules of behavior to supplement Agency level rules are not adequate;

(c) Develop and maintain a security Concept of Operations (CONOPS) for the information system containing at a minimum, how the system is intended to operate from the perspective of information security;

(d) Develop and maintain security architecture documents that describe:

(1) The overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;

(2) How the information security architecture is integrated into and supports the enterprise architecture;

(3) Any information security assumptions about, and dependencies on, external services.

(e) Determine how the system will integrate into common controls that are centrally managed by the Peace Corps Enterprise.

6.1.13 Program Management (PM) Policy

An Enterprise Information Security Program plan shall be developed by the CISO to improve Peace Corps security practices across the enterprise.

System owners will comply with Enterprise Information Security Program plan and implement sub controls that are determined to applicable to their system.

6.1.14 Personnel Security (PS) Policy

In accordance with the PS Control baseline defined by the system's categorization, ISSOs in support of system owners will:

(a) Coordinate with Safety and Security, who have responsibility for risk and sensitivity designations for all positions, to ensure the appropriate level of designation is established for all system and mission level positions and establish screening criteria if additional screening is required beyond what is executed in the Peace Corps onboarding process;

(b) Ensure user provisioning and de-provisioning process and procedures are in place the system and mission level that are adequate to track users employment status and take the necessary user account actions in a timely manner; and

(c) Ensure individuals that require access complete access agreements prior to granting access.

6.1.15 Risk Assessment (RA) Policy

In accordance with the RA Control baseline defined by the system's categorization, ISSOs, in support of System Owners, will:

(a) Complete a FIPS 199, Privacy Threshold Analysis and e-Authentication risk assessment for information systems in accordance with the Agency's implementation of the RMF;

(b) Conduct, document and maintain an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

(c) Conduct vulnerability scanning and remediate findings in a timely manner in accordance with Agency requirements.

6.1.16 System Services Acquisition (SA) Policy

In accordance with the SA Control baseline defined by the system's categorization, Security Policy & Governance (SP&G), on behalf of System Owners, will:

(a) Determine and document information security requirements for the information system or information system service in mission/business process planning;

(b) Allocate the proper resources required to protect the information system or service as part of the capital planning and investment control process;

(c) Define and document security roles and responsibilities throughout the System Development Life Cycle;

(d) Includes the all requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and mission/business needs;

(e) Ensure that appropriate information system security engineering principles are applied in the specification, design, development, implementation, and modification of the information system;

(f) Requires that providers of external information system services comply with Peace Corps information security requirements in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

(g) Ensure appropriate developers controls are applied during the development and implementation of a system or component.

6.1.17 System and Communication Protection (SC) Policy

In accordance with the SC Control baseline defined by the system's categorization, ISSOs, on behalf of System Owners, will ensure that adequate system and communications protections are implemented that comply with the Peace Corps Cybersecurity and Privacy Catalog.

6.1.18 System and Information Integrity (SI) Policy

In accordance with the SI Control baseline defined by the system's categorization, ISSOs, on behalf of System Owners, will ensure that adequate system and communications protections are implemented that comply with section 3.18 of this document.

6.2 Privacy Control Policies

For Privacy Controls Policy see MS 897. For Cybersecurity controls related to Privacy see the Cybersecurity and Privacy Catalog.

6.3 Agency and Issue Specific Policies

Issue-specific policies state Peace Corps **unclassified** information security policy for specific areas interest, like cloud use and mobile devices. These issue-specific policies span the entire Agency and often contain unique technology position statements.

6.3.1 Encryption Requirements

(a) All agency website and service available over the Hypertext Transfer Protocol (HTTP) connections must enable and utilize the HTTP Strict Transport Security (HSTS).

(b) All agency websites and services used for secure data transmission will implement Transport Layer Security (TLS) 1.2 or higher. Legacy systems that do not support TLS 1.2 or higher may be exempted.

(c) There are no encryption requirements for low impact information.

(d) Moderate and high impact information is considered sensitive information and must be encrypted in accordance with FIPS 140-2.

(e) High impact information must be encrypted while at rest or in storage in accordance with FIPS 140-2.

(f) Agency furnished and Bring Your Own Device (BYOD) mobile devices must have FIPS 140-2 encryption and containerization capabilities.

6.3.2 Third Party Collaboration Tools and Cloud Services

Peace Corps staff may use OCIO approved third party collaboration tools to enable work directly with external partners, contacts or Peace Corps Volunteers only in circumstances in which there is low impact information. All third party collaboration tools must be approved by the OCIO Security Policy & Governance prior to being used to conduct Peace Corps related business. These tools cannot be used to transmit, aggregate, share or store moderate or high impact, or sensitive information.

In addition, in order to address federal IT cybersecurity and record keeping concerns, the OCIO must expressly approve in writing any proposed software programs used via Cloud Services or otherwise on Peace Corps information systems and hardware, including but not limited to desktop and laptop computers and mobile devices. The OCIO will provide instructions to Peace Corps staff and other users on how to seek appropriate approval. **Unapproved Cloud Services including software programs downloaded from the Cloud by Peace Corps staff and other**

users may be removed by the OCIO immediately without notice from Peace Corps information systems and hardware.

All staff created, maintained or retained content on third party collaboration tools including Cloud Services are subject to FOIA disclosure and must follow Federal records management laws and requirements as is done with all agency records. Federal records must also be stored in an appropriate location within the Peace Corps environment by staff users who must export documents or media from the third party collaboration tools until the process can be automated.

7.0 Policy Deviations

The Chief Information Security Officer (CISO), Risk Executive, and the Authorizing Official must approve cybersecurity policy deviations. Cybersecurity policy deviation requests will be submitted to OCIO Security Policy & Governance by a Department Director or higher and documented through the POA&M management process.

It is Peace Corps policy that personnel and **unclassified** information systems abide by or exceed the requirements outlined in this policy and the associated procedures for each NIST SP 800-53 family of controls documented in the Peace Corps Cybersecurity and Privacy Catalog. SP&G will assess Peace Corps' adherence with this document through various oversight and compliance measures.

Individuals found to be non-compliant with this policy may be subject to a review in accordance with the following:

(a) Employee discipline under MS 647.

(b) Contractor suspension or debarment.

(c) Removal of an individual's authority to access Peace Corps information systems.

(d) Peace Corps information systems are required to have a current Security Authorization – To-Operate (ATO) designated by an Authorizing Official. A system that is found to be non-compliant with this policy will be subject to CIO review and possible removal from network.

8.0 Procedures

The Cybersecurity and Privacy Catalog (CPC) provides the procedures and organization defined parameters (ODP) required under law to implement **unclassified** information security policies. All changes to the CPC are developed by the OCIO and reviewed and approved by the Office of General Counsel. Country Directors may issue additional country-specific procedures for information technology accessing the Peace Corps network, provided they are consistent with this Manual Section. Any such country-specific procedures must be approved by the CISO and OGC prior to their effective date.

9.0 Effective Date

The effective date is the date of issuance.